In re Application of:
Christopher L. Hamlin
Serial No.: 09/630,069
Filed: 07/31/00
Title: A COMPUTER NETWORK COMPRISING NETWORK AUTHENTICATION FACILITIES IMPLEMENTED IN A DISK DRIVE

Group Art Unit: 2134
Examiner: Tran, Ellen C.

BRIEF ON APPEAL

THE COMMISSIONER FOR PATENTS
ALEXANDRIA, VA 22313

Sir,

The following appeal brief is submitted pursuant to the Notice of Appeal filed on 9/07/04, in the above-identified application.

REAL PARTY IN INTEREST

The real party in interest for the above-identified patent application is Western Digital Technologies, Inc. (see assignment REEL/FRAME: 011901/0033 identifying Western Digital Technologies, Inc. as assignee of the entire right, title and interest of the above-identified patent application).

RELATED APPEALS AND INTERFERENCES

There are no known appeals or interferences related to the instant appeal.

STATUS OF CLAIMS

Claims 1-26 are the only claims pending and stand under final rejection. Claims 1-26 are the basis of this appeal.

STATUS OF AMENDMENTS

There are no outstanding amendments.

SUMMARY OF INVENTION

FIG. 2 shows a computer network according to an embodiment of the present invention as comprising a plurality of interconnected network devices including a plurality of client computers 18, an authentication server computer 24 operated by a system administrator 12, and a disk drive 22 connected to the authentication server computer 24. FIG. 3 shows a disk drive 21 according to an embodiment of the present invention for use as the disk drive 22 connected to the authentication server computer 24 in the computer network of FIG. 2. The disk drive 21 comprises an interface 28 for receiving personal authentication data 26 and user access data 30 from the system administrator 12, a disk 32 for storing data, and a disk controller 34 for controlling access to the disk 32. An authenticator 36 within the disk drive 21, responsive to the personal authentication data 26, enables the disk controller 34, and cryptographic circuitry 38 within the disk drive 21 encrypts the user access data 30 received from the authentication server computer 24 into encrypted data 40 stored on the disk 32.

ISSUES

I. Whether claims 1-5, 7, 9, and 11-17 are patentable under 35 USC §102(e) over Alonso et al. (6,434,700).

II. Whether claims 6, 8, 10, 18-26 are patentable under 35 USC §103(a) over Alonso in view of DeTreville (6,609,199).

GROUPING OF CLAIMS

Claims 1-26 stand rejected and are grouped together for the purpose of this appeal.

THE REFERENCES

The following references are relied upon by the examiner:

Alonso et al.	6,434,700	Aug. 13, 2002
DeTreville	6,609,199	Aug. 19, 2003

THE REJECTIONS

Claims 1-5, 7, 9, and 11-17 stand rejected under 35 USC §102(e) as anticipated by Alonso et al.. The examiner asserts Alonso discloses network authentication facilities implemented within a disk drive.

Claims 6, 8, 10, and 18-26 stand rejected under 35 USC §103(a) as unpatentable over Alonso et al. in view of DeTreville. The examiner asserts that because DeTreville teaches the use of a secrete device key, the authorization access server disclosed by Alonso could be modified to include a secrete device key.

INTERVIEW SUMMARY

On 09/01/04 the applicant held a telephone interview with the examiner to discuss the rejections in the final office action. The applicant explained how Alonso teaches to use a network access server to implement the authentication facilities for authenticating the user. The examiner relied on col. 6, lines 16-17, to support the assertion that Alonso teaches to implement

the authentication facilities in a disk drive. The examiner also sustained the rejection arguing that Alonso teaches at col. 2, lines 6-13, a Fortezza security card for authenticating the user which renders obvious the applicant's invention wherein the authentication facilities are implemented within a disk drive.

ARGUMENT

I. THE ISSUE UNDER 35 U.S.C. §102(e) – ALONSO

A. The rejection should be reversed because Alonso teaches to implement authentication facilities in a network access server or access control server rather than in a disk drive.

The rejection should be reversed because the examiner has incorrectly construed Alonso as teaching to implement user authentication facilities within a disk drive.

The examiner asserted in paragraph 8 of the final office action that the Fortezza Crypto card disclosed by Alonso authenticates the user of a network. This interpretation of Alonso is incorrect. Although Alonso teaches that the Fortezza Crypto card generates and authenticates one-time passwords (OTPs), the Fortezza Crypto card does not authenticate the user. Instead, Alonso discloses that the OTP and user access information are sent to a network access server (Fortezza server 114) which "determines if the user 106 is authorized to access the network 108 and what set of access privileges the user 106 is allowed to obtain." (See col. 3, lines 21-44). Therefore, Alonso teaches that a network access server and not the Fortezza Crypto card authenticates the user. Alonso also teaches an access control server (ACS) for implementing user authentication facilities, but nowhere does Alonso disclose or suggest to implement user authentication facilities within a disk drive as recited in the claims.

In rejecting claims 6, 8, 10, and 18-26 discussed below, the examiner asserted on page 7 (paragraph 2) of the final office action that the access control server (ACS) disclosed by Alonso could be modified in view of DeTreville to include a secrete device key. Thus, the examiner appears to agree with the applicant that Alonso discloses an access control server for implementing the user authentication facilities rather than a disk drive. The rejection should therefore be reversed.

II. THE ISSUE UNDER 35 U.S.C. §103(a) – ALONSO IN VIEW OF DETREVILLE

A. The rejection should be reversed because Alonso teaches to implement authentication facilities in a network access server or access control server rather than in a disk drive.

Claim 22 recites a disk drive comprising an interface for receiving an encrypted device access request and for inputting/outputting user data from/to a client computer. The disk drive further comprises an internal drive key and an encrypted secrete device key shared with an authentication server. Cryptographic circuitry in the disk drive decrypts the encrypted secrete device key using the internal drive key to generate a decrypted secrete device key. The disk drive comprises an authenticator for authenticating the device access request using the decrypted secrete device key.

The examiner asserts that because DeTreville teaches the use of a secrete device key, the access control server disclosed by Alonso could be modified to include a secrete device key. However, modifying Alonso in view of DeTreville would result in an access control server implementing network authentication facilities using a secrete device key and not a disk drive implementing authentication facilities using a secrete device key. Further, DeTreville discloses in FIG. 3 a computer 118 for implementing authentication facilities using a secrete key and

therefore does not disclose or suggest to implement authentication facilities within a disk drive.

The rejection should therefore be reversed.

CONCLUSION

Reversal of the rejections in this appeal is respectfully requested.

To the extent necessary, a petition for an extension of time under 37 C.F.R. 1.136 is hereby made. Please charge any shortage in fees due in connection with the filing of this paper, including extension of time fees, to Deposit Account No. 23-1209, and please credit any excess fees to such deposit account.

Respectfully submitted,

Date: 12/7/04 By: _____

Howard H. Sheerin
Reg. No. 37,938
Tel. No. (303) 765-1689

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Commissioner of Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on:

12/7/04 Howard H. Sheerin
(Date) (Print Name)

_____
(Signature)

APPENDIX

A complete listing of the claims on appeal:

1. A computer network comprising a plurality of interconnected network devices including:
   (a) a plurality of client computers;
   (b) an authentication server computer operated by a system administrator; and
   (c) a disk drive connected to the authentication server computer, the disk drive comprising:
      an interface for receiving personal authentication data and user access data from the system administrator;
      a disk for storing data;
      a disk controller for controlling access to the disk;
      an authenticator, responsive to the personal authentication data, for enabling the disk controller; and
      cryptographic circuitry for encrypting the user access data received from the system administrator into encrypted data stored on the disk.

2. The computer network as recited in claim 1, wherein the user access data comprises a plurality of user identifiers and corresponding access rights to the plurality of network devices.

3. The computer network as recited in claim 2, wherein the user access data further comprises user authentication data.

4. The computer network as recited in claim 3, wherein the user authentication data comprises a user password.

5. The computer network as recited in claim 1, wherein the personal authentication data comprises a user password.

6. The computer network as recited in claim 1, wherein:
(a) the cryptographic circuitry comprises an immutable secret drive key configured during manufacture of the disk drive; and
(b) the secret drive key for use in encrypting the user access data.

7. The computer network as recited in claim 2, wherein:
(a) the disk stores encrypted device access data associated with the network devices; and
(b) the device access data for use in authenticating device access requests transmitted from client computers to the network devices.

8. The computer network as recited in claim 7, wherein the encrypted device access data comprises an encrypted secret device key shared with a corresponding network device.

9. The computer network as recited in claim 7, wherein:
(a) the interface receives unencrypted device access data; and
(b) the cryptographic circuitry encrypts the unencrypted device access data into the encrypted device access data stored on the disk.

10. The computer network as recited in claim 7, wherein the encrypted device access data is stored on the disk during manufacture of the disk drive.

11. The computer network as recited in claim 7, wherein the encrypted device access data is transmitted from the network devices to the disk drive.

12. A computer network comprising a plurality of interconnected network devices including:
(a) a plurality of client computers;
(b) an authentication server computer; and
(c) a disk drive connected to the authentication server computer, the disk drive comprising:
an interface for receiving from a client computer a user ID and a user access request to access a network device, and for transmitting device access data to the client computer;
a disk for storing encrypted data;
a disk controller, responsive to the user ID and user access request, for controlling access to the disk; and
cryptographic circuitry for decrypting the encrypted data stored on the disk to generate decrypted data,
wherein the disk controller uses the decrypted data to generate the device access data transmitted to the client computer.

13. The computer network as recited in claim 12, wherein:
(a) the encrypted data comprises encrypted user authentication data corresponding to the user ID; and
(b) the cryptographic circuitry decrypts the encrypted user authentication data to generate decrypted user authentication data.

14. The computer network as recited in claim 13, wherein the decrypted user authentication data comprises a user password.

15. The computer network as recited in claim 12, wherein the cryptographic circuitry encrypts the device access data before transmission to the client computer.

16. The computer network as recited in claim 13, wherein:

(a) the cryptographic circuitry encrypts the device access data before transmission to the client computer; and

(b) the cryptographic circuitry encrypts the device access data using a cryptographic user key extracted from the decrypted user authentication data.

17. The computer network as recited in claim 16, wherein the cryptographic user key is generated by the cryptographic circuitry using the decrypted user authentication data.

18. The computer network as recited in claim 16, wherein the cryptographic user key is a public key for use in a public key encryption algorithm.

19. The computer network as recited in claim 12, wherein:

(a) the cryptographic circuitry encrypts the device access data using a secret device key shared with the network device; and

(b) the secret device key is used by the network device to authenticate device access requests received from client computers.

20. The computer network as recited in claim 19, wherein the secret device key shared with the network device is stored in encrypted form on the disk and decrypted by the cryptography circuitry.

21. The computer network as recited in claim 12, wherein:

(a) the cryptographic circuitry comprises an immutable secret drive key configured during manufacture of the disk drive; and

(b) the secret drive key for use in decrypting the encrypted data stored on the disk.

22. A computer network comprising a plurality of interconnected network devices including:

(a) a plurality of client computers;

(b) an authentication server; and

(c) a disk drive comprising:

an interface for receiving an encrypted device access request and for inputting/outputting user data from/to a client computer;

a disk for storing data;

a disk controller for controlling access to the disk;

an internal drive key;

a secret device key shared with the authentication server, the secret device key stored in encrypted form;

cryptographic circuitry, responsive to the internal drive key, for decrypting the encrypted secret device key to generate a decrypted secret device key; and

an authenticator, responsive to the decrypted secret device key, for authenticating the device access request.

23. The computer network as recited in claim 22, wherein the encrypted secret device key is stored on the disk.

24. The computer network as recited in claim 22, wherein the encrypted secret device key is configured during manufacture of the disk drive.

25. The computer network as recited in claim 22, wherein the disk drive transmits the encrypted secret device key to the authentication server.

26. The computer network as recited in claim 22, wherein the internal drive key comprises tamper-resistant circuitry.